Program Research Project

ACHIEVING DOD'S NET CENTRIC VISION OF INFORMATION SHARING WHILE OVERCOMING CULTURAL BIASES TO CONTROL INFORMATION

BY

CAPTAIN PAUL M. SHAW
United States Navy Reserve

USAWC CLASS OF 2008

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

Prudens Futuri

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **09 MAY 2008**	2. REPORT TYPE **Program Research Paper**	3. DATES COVERED **00-00-2007 to 00-00-2008**

4. TITLE AND SUBTITLE
Achieving DoD’s Net Centric Vision of Information Sharing While Overcoming Cultural Biases to Control Information

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Paul Shaw

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**26**	

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 09-05-2008	**2. REPORT TYPE** Program Research Paper	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Achieving DoD’s Net Centric Vision of Information Sharing While Overcoming Cultural Biases to Control Information	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Captain Paul M. Shaw, USNR	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) COL(RET) Robert Smith Department of Distance Education	**10. SPONSOR/MONITOR’S ACRONYM(S)** **11. SPONSOR/MONITOR’S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A: UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Global War on Terrorism and countering other threats is increasingly dependent upon better information sharing within and between agencies. US national and agency information sharing strategies promote culture change as a critical enabler. A culture change from a “need to know” to a “need to share” is the desired end state. This culture change is in contrast to known organizational and individual cultural biases to control information. Within the DoD, key policies like the Net Centric Data Strategy (NCDS) promote accessibility. Other policies then place information assurance requirements upon implementers that allow interpretation for what to share. Instead of curtailing cultural biases and furthering desired information sharing objectives, this policy tension between accessibility and information assurance enables information control. DoD policy as a part of DoD’s ways and information sharing technology as part of DoD’s means are examined using the USAWC Strategy Model of “ends, ways, and means.” Modifications to the DoD’s NCDS and other policies could counter known cultural biases and accommodate cultural differences.

15. SUBJECT TERMS

Semantic Web, Key Policies

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	26	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC PROGRAM RESEARCH PROJECT

ACHIEVING DOD'S NET CENTRIC VISION OF INFORMATION SHARING WHILE OVERCOMING CULTURAL BIASES TO CONTROL INFORMATION

by

Captain Paul M. Shaw
United States Navy Reserve

Topic Approved By
Colonel (Retired) Robert Smith

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	Captain Paul M. Shaw
TITLE:	Achieving DoD's Net Centric Vision of Information Sharing While Overcoming Cultural Biases to Control Information
FORMAT:	Program Research Project
DATE:	9 May 2008 WORD COUNT: 4,750 PAGES: 26
KEY TERMS:	Semantic Web, Key Policies
CLASSIFICATION:	Unclassified

The Global War on Terrorism and countering other threats is increasingly dependent upon better information sharing within and between agencies. US national and agency information sharing strategies promote culture change as a critical enabler. A culture change from a "need to know" to a "need to share" is the desired end state. This culture change is in contrast to known organizational and individual cultural biases to control information. Within the DoD, key policies like the Net Centric Data Strategy (NCDS) promote accessibility. Other policies then place information assurance requirements upon implementers that allow interpretation for what to share. Instead of curtailing cultural biases and furthering desired information sharing objectives, this policy tension between accessibility and information assurance enables information control. DoD policy as a part of DoD's ways and information sharing technology as part of DoD's means are examined using the USAWC Strategy Model of "ends, ways, and means." Modifications to the DoD's NCDS and other policies could counter known cultural biases and accommodate cultural differences.

ACHIEVING DOD'S NET CENTRIC VISION OF INFORMATION SHARING WHILE OVERCOMING CULTURAL BIASES TO CONTROL INFORMATION

> "We can not use the same thinking to solve the problem that caused the problem."
>
> Albert Einstein

Among US national security strategies, information sharing has a prominent role in combating terrorism and other threats through improved situational awareness, actionable intelligence, and better decision making. To achieve desired information sharing, the US Executive Branch and numerous government agencies, including the Department of Defense (DoD), Director of National Intelligence (DNI), Department of Homeland Security (DHS), and Department of Justice (DOJ), have information sharing strategies. All of these agencies' strategies endorse a change of culture from a "need to know" to a "need to share" to promote information sharing objectives. These mandates for culture change are strong with broad, encompassing objectives. Why does the Government Accounting Office (GAO), along with other oversight agencies, find the US government not achieving desired effects?[1] Cultural issues are a key problem. The 2007 U.S. Army War College Key Strategic Issues List (KSIL) Army G6 question of how to "achieve DoD's netcentricity vision of ubiquitous access in light of the cultural biases among people and organizations to control information"[2] is a core issue. Can the DoD either change policy, develop collaboration capabilities, or perform both to promote information sharing and overcome cultural bias to control information?

A review of DoD information sharing policies along with an examination of ways and means might be a way to understand and determine appropriate courses of action. Policy change could be a significant enabler to promote net centric enablement and achieve desired information sharing effects. Policy can fail if it ignores Einstein's advice of using the same thinking to create and solve the problem or provides conflicting guidance for the implementer to resolve. Does the DoD's Net Centric Data Strategy (NCDS) have these failure criteria? Should the DoD's NCDS policy of sharing of all information "except where limited by law, policy, or security classification"[3] be modified to prevail over cultural biases to control information? In modifying DoD key policies to accommodate cultural biases, can the DoD leverage the rules of successful cultural interaction and develop collaboration capabilities to overcome information control bias? Other options to counter cultural bias for information control are a means issue dealt with by evolving technology.

The author examines the DoD information control problem using the U.S. Army War College (USAWC) Strategy Model of "ends, ways, and means." In the USAWC Strategy model, ends equal objectives; ways equal concepts; and means equal resources.[4] This information control problem could have issues in its scope of objectives, policies for ways, and technology for means. In the USAWC Strategy Model, reduction of objectives can be a way to achieve a balance between ends, ways, and means. As US national security strategy and information sharing documents show a progression of desired information sharing capabilities, desired ends may allow little latitude in reduction of information sharing objectives. Either modifying policy as a way or using better technology as a means might be an effective strategy to achieve desired effects and to reduce risk. Tim Berners-Lee, founder of the World Wide Web, said, "it is essential that policy and technology be designed with a good understanding of the implications of each other."[5] Changing ways and means is a viable option for understanding and addressing DoD's cultural biases. The USAWC Strategy Model helps to determine if modification of ways or means promotes improved information sharing.

Policy

US national security strategies display a range of information sharing objectives. The National Security Strategy of the United States (NSS) uses information sharing as a way to improve intelligence and its use.[6] The National Strategy for Maritime Security (NSMS) strives for "full and complete national and international coordination, cooperation, and intelligence and information sharing among public and private entities." NSMS Information sharing calls for "timely, credible, and actionable intelligence" as an enabler for "situational awareness and integrated command and control."[7] The National Military Strategy to Combat Weapons of Mass Destruction has information sharing in the mission thread for stopping WMD proliferation.[8] The National Strategy for Information Sharing and agency sharing strategies, such as DoD Information Sharing Strategy, United States Intelligence Community Information Sharing Strategy, and LEISP: United States Department of Justice Information Sharing Plan, are among a series of information sharing strategies to achieve these effects. The combined set of security strategies and information sharing strategies create a framework and US desired objectives. Critical to notice is that US desired ends are increasing in scope and importance, which supports the earlier comment on the USAWC Strategy Model. Ends reduction may be the least acceptable option to balance any ends, ways, and means imbalance.

The DoD core policies promoting data accessibility are DoD Directive 8320.2 "Information Sharing in a Net-Centric Department of Defense" and DoD Directive 8320.02-G "Guidance for Implementing Net-Centric Data Strategy." This accessibility is balanced with US directives on information assurance such as DoD Directive 8500.1 "Information Assurance" and DoD Directive 4630.5 "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" for information assurance requirements. To promote data availability, DoD Directive 8320.2 (NCDS) states "4. POLICY- It is DoD policy that: …4.3. Data assets shall be made accessible by making data available in shared spaces. All data assets shall be accessible to all users in the Department of Defense except where limited by law, policy, or security classification."[9] DoD Directive 8320.02-G provides "for governing and managing the development of new data sharing capabilities."[10] Its key capabilities revolve around making data visible, accessible and understandable, along with promoting trust.

This accessibility is countered by DoD Directive 8500.1 requirements for DoD IT systems to maintain information assurance. "This combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response."[11] DoD Directive 4630.5 ensures interoperability of IT systems throughout the DoD. "IT and NSS, of the DoD Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare."[12]

DoD Directive 8320.02-G uses Communities of Interest (COIs) as collaborative user groups who "exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange."[13] COIs are responsible for developing data architecture within a particular context. In DoD Directive 8320.02-G, COIs identify authoritative data sources (ADS). These ADS are "data assets that are authoritative sources for data."[14] Data producers, who are members of COIs, have the responsibilities to "make data assets accessible using web-based approaches"[15] This concept of COIs, ADS, and data producers is more about data structure, assets, and accessibility. It lacks the responsibilities that data producers should have to share, especially authoritative data producers, and does not counter the cultural bias to control information.

Requirements for privacy, access, and ownership come from tasks, processes, laws, and policy. The Privacy Act of 1974 is an example of a law that imposes requirements on information exchange. The Privacy Act regulates the government's collection, maintenance, use, and dissemination of information on people. Its goal is to protect individual privacy rights of United States citizens and permanent legal residents. Under the Privacy Act, agencies must ensure that records with privacy information are accurate and complete. Agencies have a responsibility for allowing individuals access to their records for review of information.[16] Privacy information can require special validation processes to ensure accuracy, timeliness, consistency, and completeness, such as reconciliation keys and specialized metadata.

Federal Information Processing Standards (FIPS) 199 is titled the “Standards for Security Categorization of Federal Information and Information Systems.”[17] FIPS 199 is a government wide framework for understanding the risk of undesired information disclosure or system breach. Information and systems can have a security categorization. FIPS 199 allows analysis for risk of a security breach, adequacy of security objectives, and determination of a security categorization. The overall combination of these themes helps to assign the risk impact level of information and system compromise. Impact could range from minimal effect to embarrassment to hostile response. Balancing confidentiality, integrity, and availability are part of the FIPS 199 categorization. The combination of the impact in connection with information classifications help to determine the overall security categorization. These categorizations of system and information are in context of the organization mission, legal responsibilities (such as the Privacy Act), asset and people protection, and threat.

It would seem that the NCDS’ simple policy of “share all” would transform the DoD culture from a “need to know” culture to a “need to share” in one simple stroke. Yet this policy allows wide implementation interpretation for the “where limited by law, policy, or security classification,” especially with US concepts for risk of information disclosure in FIPS 199 and other policy information assurance requirements. In the DoD, the current NCDS policy sharing strategy does not adequately address DoD’s cultural biases among people and organizations to control information. Across DoD policies, the ability to implement information access has wide latitude for interpretation and a balancing tension between requirements. Allowing such interpretation has not worked for achieving information sharing objectives due to cultural biases at the organizational and individual levels. The range of the cultural biases showed up in its various 2007 KSIL questions about culture and information sharing. In violation of Einstein's advice, the DoD NCDS is using similar thinking to cause and solve the problem The DoD NCDS accommodation of "where limited by"[18] creates part of the enablement for cultural bias information control. Options for policy change are presented with a recommended course of action.

DoD's Cultural Biases

While there are many different definitions of culture, the following definition frames this evaluation:

> A set of values, symbols and rituals shared by the members of a specific firm, which describes the way things are done in an organization in order to solve both internal management problems and those related to customers, suppliers and the environment. …Culture manifests itself at both a visible level (age, ethnicity, gender, dress, organizational structure, symbols, slogans, etc.) and an invisible level (time, motivation, stability vs. change, orientation towards work, individualism vs. collaboration, control, how management views IT, etc.).[19]

Precise agreement on culture's definition is less important than examining and understanding the below organizational and individual biases manifested through culture.

There are cultural biases between organizations, where respective cultures have to interact with each other. A cultural bias could be a result of an organization's responsibility to protect certain types of information, due to either legal, moral, or agency mission requirements. Organizations have a fear of misuse of their data, sometimes with severe external consequences. Competition between agencies can create a cultural bias, especially when forced to work with each other. DHS in their unification of capability across 22 distinct agencies[20] experienced an issue for the time and effort to develop points of integration and revise information processes. Melding agencies is a common mistake when agencies start sharing common organizational purpose and goals, instead of determining points of integration and responsibilities for information sharing. This may force agencies into a structure preservation mode of trying to preserve understood relationships. "This kind of a structure-preserving relationship between two sets of things is called a *homomorphism*."[21] A false sense of agency loyalty can impede use of other agency information. Legacy systems create an organizational cultural bias of systems and technology, especially when such legacy systems have to undergo a modification to accommodate information sharing. The lack of policy, doctrine, and process modification create a ways issue to understand the cross agency points of integration and methods of sharing. Legacy technology is a means issue.

Individual bias against information sharing could be a variety of issues. The bias for information control could be at the individual level due to desires to hoard information for reasons of power, influence, importance, job security, and reward. Individual information control could be from desire to personally create a product, which could be either from the lack of ability to collaborate or resource constraints. Individuals may have problems sharing products due to limitations of legacy systems. Some organizations have configuration control procedures in place to ensure only final versions are available and prevent individuals from sharing multiple product versions. Increasingly DoD systems provide information overload due to the volume of available information. A natural temptation of an individual performing a task is to seek out additional information until information overload exceeds their comprehension limits. Either an individual reduces available information and succeeds, or is overwhelmed. Many previous DoD information sharing efforts were dependent upon personal relationships, with skilled and experienced people knowing how to work around the system to be able to get the right answer.

Individual and organizational risk aversion reinforces DoD's cultural bias for control information. Criticism or punishment is normal for the individual or organization deemed to inappropriately share due to a legal, moral, or classification issue. Rarely is an organization or individual punished for not sharing information. Even in the thorough reviews of major events like 9-11, proving an organization or individual should have shared information is difficult.

Respecting Culture

"When efforts to implement change fail, a common cause is insufficient attention to the people-side of change. …treat information as a resource (on par with human resources, financial resources, physical resources) and consider how they can change the organization's information culture first through the people-side of change."[22] A starting point for the "people-side of change" would be respecting cultures, acknowledging cultural biases, and developing more effective policies and technology. Respecting culture could embody many things at both organizational and individual levels. Some of the best rules for promoting information sharing come from the following rules for successful cultural interaction by Prof. Carlos Cortés.

1. Draw upon the strengths of diversity in order to work toward common organizational goals.

> 2. Create a climate in which members of the organization feel welcomed to draw upon their diverse cultures and experiences, without feeling obligated to constantly represent “their people.”
>
> 3. Draw constructively and flexibly on knowledge about groups, while using that knowledge as a clue, not as an assumption about individuals.
>
> 4. Distinguish between those problems that can be resolved by establishing a rule and those that will require long-range, continuous action to modify attitudes, perceptions, and behavior.
>
> 5. Accommodate constructively to diversity while also determining which accommodations are reasonable and which need to be limited.
>
> 6. Work toward both equality and organizational effectiveness by determining when it is appropriate to treat all people alike and when it is appropriate to treat them differently.[23]

Adaptation of these cultural interaction rules for information sharing is a key enabler of the desired DoD culture change. Key constructs in these rules are to deal with organizations as entities, respect the rights of individuals in US laws and understand organizational responsibilities. Successful information sharing would: work towards common organizational goals; respect personal and privileged information; work with groups without stereotyping individuals; understand when policies and processes will promote sharing responsibilities; allow for reasonable accommodations both for organizations and individuals; and understand when organizations and individuals should be treated alike and when they should be treated differently.

It would be difficult to include all of these successful information sharing constructs in policy, outside of policies promoting sharing responsibilities between organizations and process owners. Allowing organizations to define how they should interact and what are the points of integration would be a good way to adapt the DoD NCDS and information sharing policies. Information ownership, access control, classification, privacy issues, and data quality attributes are information sharing requirements. These requirements create a context of the information for information sharing and information availability, even if not complete. As organizations capture and manage these requirements, they enable information sharing culture change. Some excellent work in commercial geospatial information management in transportation and real estate illustrate this principle of information sharing requirements management.[24] The management of information legal, moral, and classification requirements is a great way to promote information sharing and lessen the fear of information disclosure persecution. Tim Berners-Lee advises, “human communication scales up only if we can be tolerant of the differences while we work with partial understanding.”[25]

The Technical Solution

Is technology a possible DoD means for culture change? Technological progress in processing speed, of greater connectivity, and for machines to work with language enables great information sharing capabilities. Complex mathematics and logic use vast data stores and a multitude of sources through continually improving processing speeds and language understandable by machines. The evolution of the World Wide Web (WWW) into the Semantic Web is one of the best places to concentrate a focus for the type of technical solutions that can change DoD culture and affect information sharing objectives.

WWW evolving Web technology offers a structure where the linkage and proximity of words would reveal patterns for development of context and understanding of meaning. The Semantic Web, Tim Berners-Lee’s follow-on to the World Wide Web, changes data to where computers could learn enough to process machine-readable data.[26] Figure 1 illustrates Tim Berners-Lee’s construct for the architecture of Semantic Web.

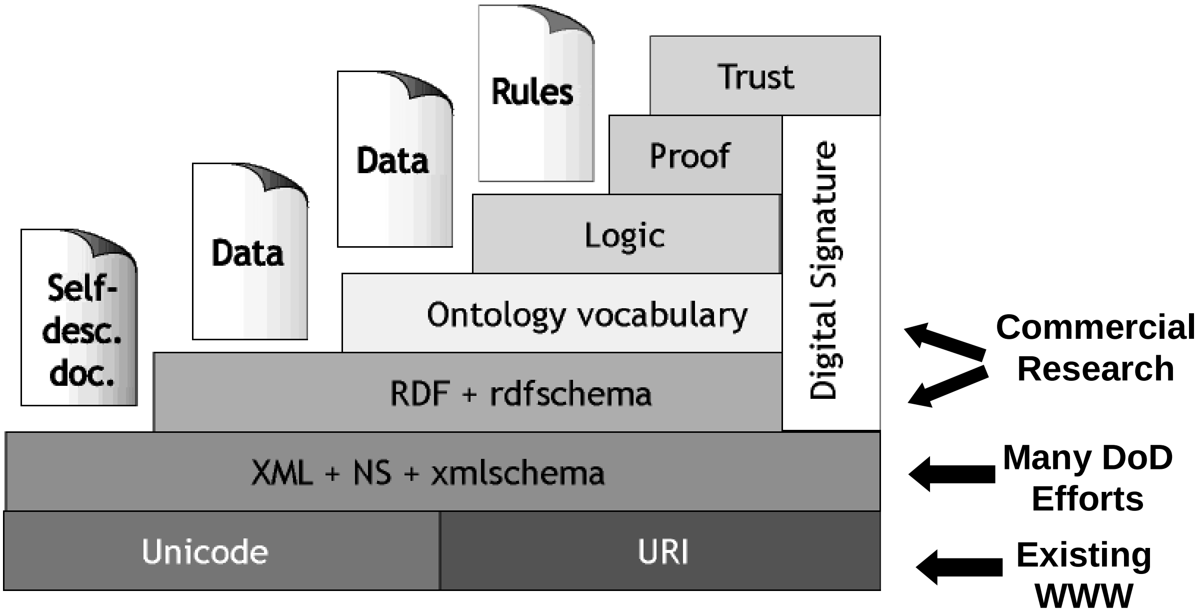


Figure 1: Slide by Tim Berners-Lee at http://www.w3.org/2000/Talks/1206-xml2k-tbl.[27] The Author added the annotation on the right side.

Current technology has different processes for how a person retrieves, uses, and stores data. These differences can affect individual bias for information control. The Semantic Web blurs the differences between these processes. This blurring starts with the Rich Description Framework (RDF) triplet concept of subject, predicate, and object. Context will increasingly be instantiated with taxonomies, schemas, metadata tags, rules and constraints, and with properties and classes through ontologies. Ontologies make language machine understandable. “Perhaps the most important contribution of the Semantic Web will be in providing a basis for the general Web’s future evolution. The consortium’s (WC3) two original goals were to help the Web maintain “interoperability” and to help it maintain “evolvability.””[28]

In DoD cultural biases, technical issues of system interoperability, collaboration, and information sharing appeared as organizational and individual issues. An over-arching data architecture or single standard for the government to define intended use and promote exploitation does not exist nor should it exist. Tim Berners-Lee advised, “making global standards is hard. The larger the number of people involved, the worse it is. In actuality, people can work together with only a few global understandings, and many local and regional ones. ….The minimalist design principle applies: Try to constrain as little as possible to meet the general goal.”[29] Information has characteristics, such as dynamic (in a state of transformation from a process or task) or static (transformations complete and at rest) and public or segmented, that may prove a range of solutions that need to be pursued. Figure 2 shows that different quadrants appear with different solutions in each quadrant. There may not be one technical solution, but instead a need for a series of solutions in the different regions.

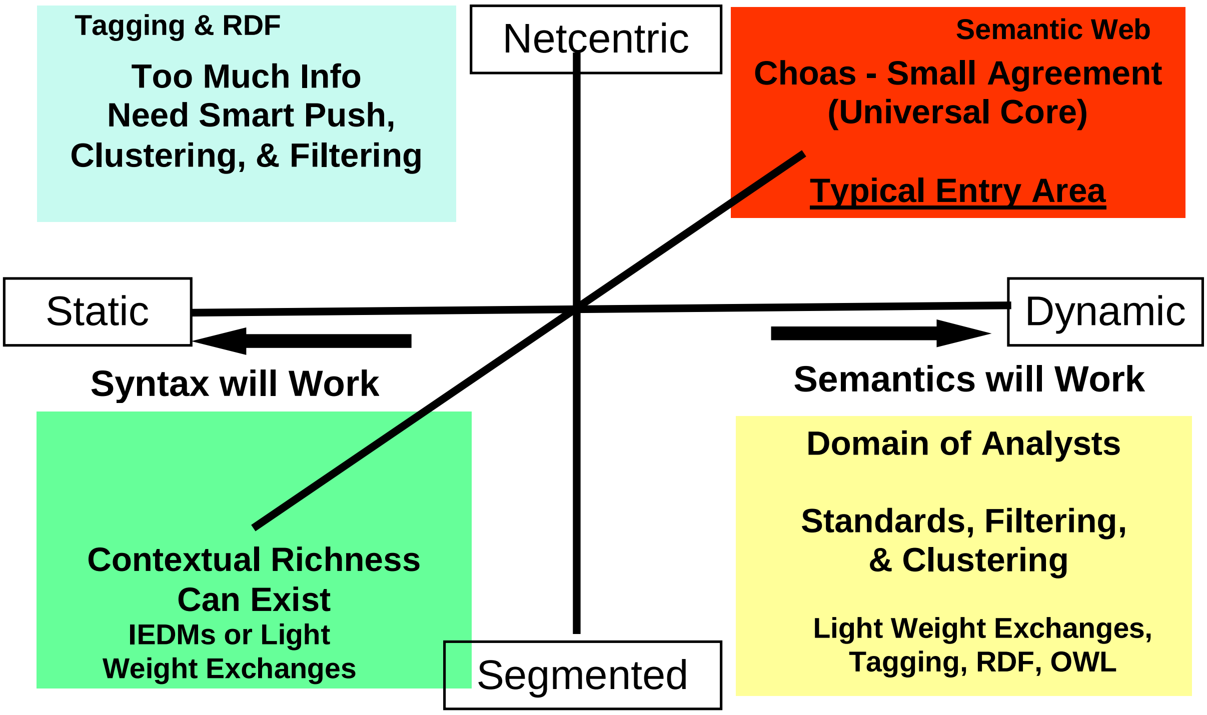


Figure 2: Information Spectrum – Even a basic classifications of the information illustrate that different strategies may exist depending on characteristics.

A key assumption in agency information sharing strategies is that key data has organizing constructs discoverable within a given context. Mission or task is organizing constructs for information classes, properties, and rules. For example, the *Intelligence Community Enterprise Architecture Data Strategy* states "data are currently created and maintained to support the specific business processes that individual organizational elements are responsible for executing."[30] Context development is a key concept for desired information fusion and dissemination in the future. Context most likely exists in layers (see Figure 3) developed over time with most information not achieving the top context layers.

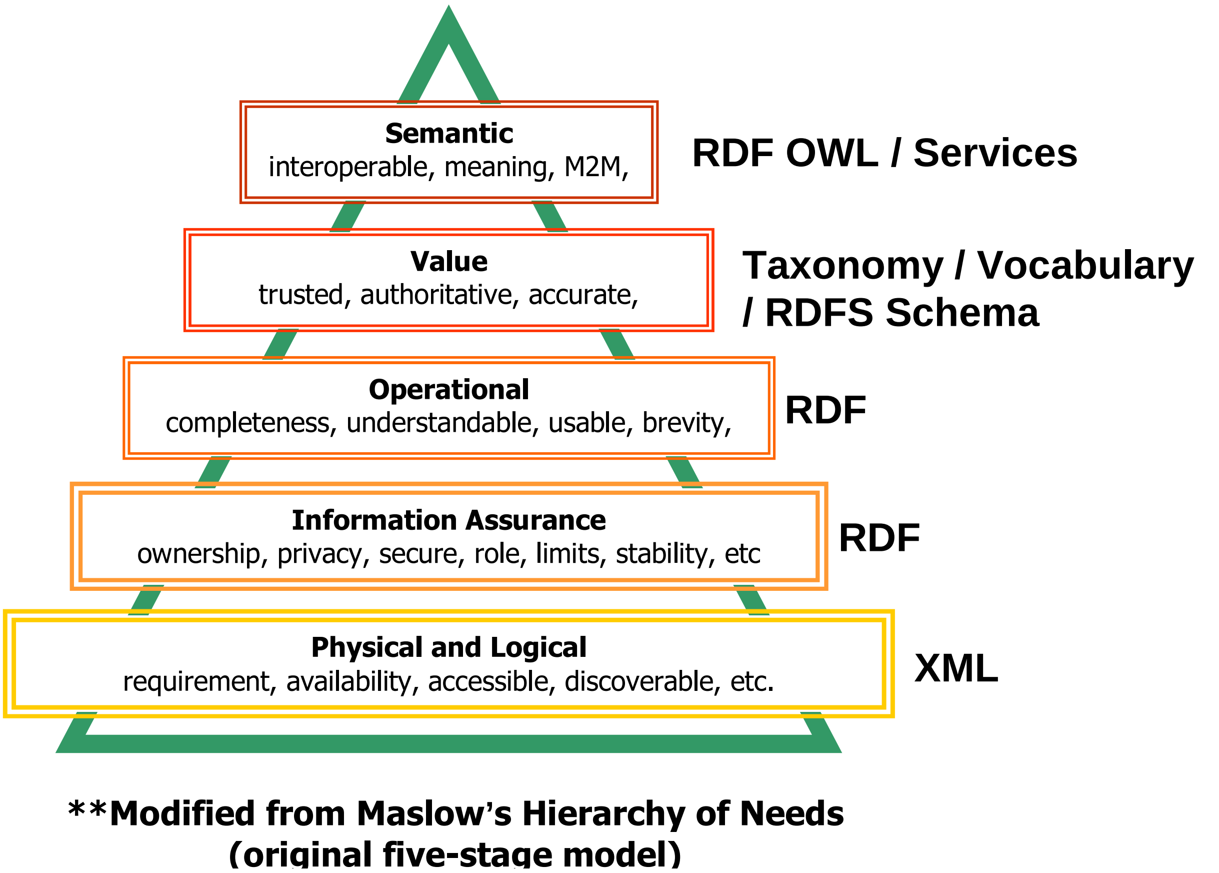
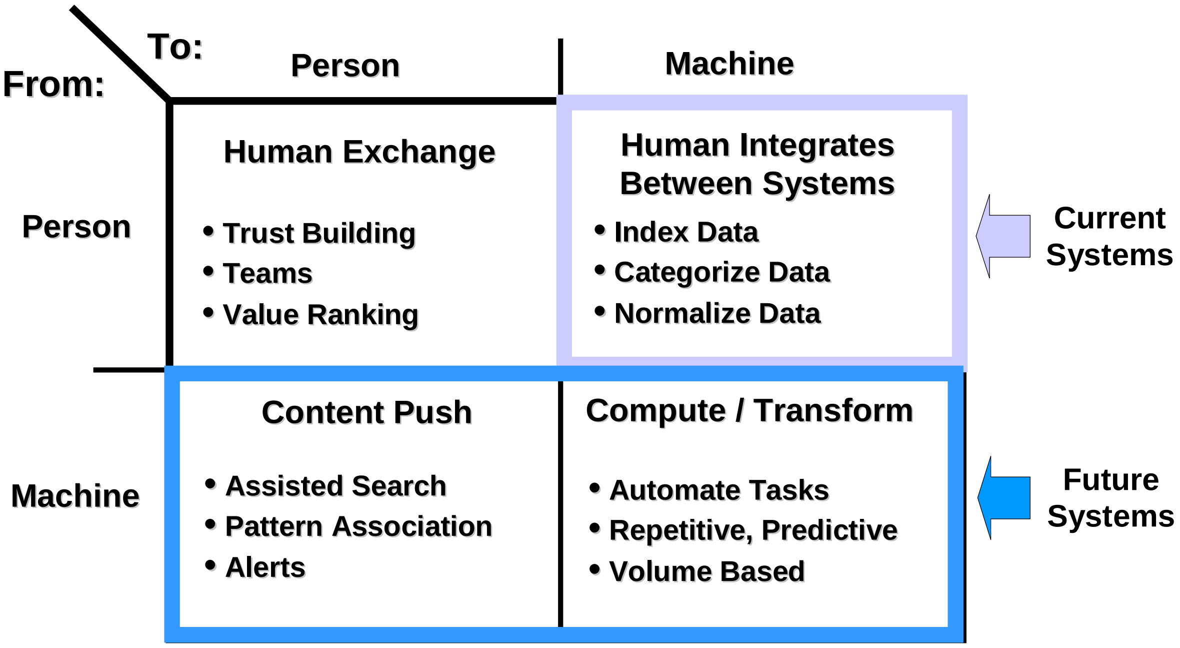

Semantic
interoperable, meaning, M2M,
RDF OWL / Services
Value
trusted, authoritative, accurate,
Taxonomy / Vocabulary / RDFS Schema
Operational
completeness, understandable, usable, brevity,
RDF
Information Assurance
ownership, privacy, secure, role, limits, stability, etc
RDF
Physical and Logical
requirement, availability, accessible, discoverable, etc.
XML
**Modified from Maslow's Hierarchy of Needs (original five-stage model)

Figure 3: Context Hierarchy – These context layers are adapted from Maslow's hierarchy by Tim Martin and Paul Shaw. The Author presented this concept at SSTC 2006 in a brief called "Semantics of Security."[31]

Many of DoD legacy systems either prevent or inhibit information sharing with others. Current information sharing integration points, such as DHS's Homeland

Security Operation Center (HSOC) for terrorism information,[32] place complex burdens on smart operators to fuse information between multiple systems. Humans are often required to find, fuse, and retype key information between systems. Technology seems to either offer many opportunities for better interaction for either machine to person or machine to machine, as illustrated in the following simple two by two grid of information flow in Figure 4.



From: \ To:	Person	Machine	
Person	**Human Exchange** • Trust Building • Teams • Value Ranking	**Human Integrates Between Systems** • Index Data • Categorize Data • Normalize Data	Current Systems
Machine	**Content Push** • Assisted Search • Pattern Association • Alerts	**Compute / Transform** • Automate Tasks • Repetitive, Predictive • Volume Based	Future Systems

Figure 4: Information Flow Grid – Most legacy systems are at the level of Person to Machine. Future systems offer Machine to Person and Machine-to-Machine capability. Dr. Dave Roberts and Paul Shaw (author) initially developed this grid. Minor modifications to the published grid are in this paper.[33]

As machines enable collaboration, people will accept the concept that they may collaborate with team members assigned by machines and that they may never meet. This dynamic is easier for younger generations to accept, especially those who have grown up with the chat and texting as acceptable social interaction. While collaboration tools are an enabler for improved information sharing, implementing the NCDS “share all” is less a technical issue than a cultural issue. Understanding when evolving technology requires human changes and the groups that might be more accepting of those changes could be a wise way to proceed now and into the future.

As the DoD continues progress towards net centricity, breakthroughs in information management and data transformation will occur. However, an over-dependence on technology is misguided and counters to desired cultural change. Concerning technology, Melvin Conway stated, ”someone someday will find a better one to do the same job. In other words, it is misleading and incorrect to speak of *the* design for a specific job, unless this is understood in the context of space, time, knowledge, and technology.”[34] If the DoD is not careful with new technologies, the DoD overwhelms users with information and negatively affects achievement of desired information sharing effects. For the near future, all government agencies are dependent upon the human and their interaction with systems. Progress in assisting users with information and knowledge management is dependent on understanding how to assist the human and not overwhelm them during this transformation. General Pace states, “I cannot yet tell you what transformation is. I am comfortable with the idea that if we had no new toys and we simply changed our mindset that we would transform significantly.”[35]

Options

I. Maintain the status quo. Continue allowing the data producer to define what to withhold in the posting of all data. Allow an ongoing tension between information assurance and information sharing. The status quo works with sensors and data sources with commodity type information, as they do a bias for control or hoarding. Current DoD policy allows users wide latitude in deciding what they can withhold due to data confidentiality and integrity requirements. Users in their roles and responsibilities self determine acceptable information control. Information control is most apparent when crossing organizational boundaries and less apparent within an organization. The current DoD environment has information sharing between systems and within processes. This option requires no changes to policy or additional resources, but lacks the ability to overcome cultural biases to control information. Status quo does not address the Army G6 KSIL question of overcoming the cultural bias to control information. Option 1 is not a viable option to achieve US national security strategies or national information sharing strategies.

II. Formalize information sharing requirements with roles and responsibilities for data producers and process owners. Formalization would impose information sharing responsibilities on process owners and data producers, especially authoritative sources. This option is preferable for key operational data sources, especially designated authoritative sources. It promotes development of information quality attributes and data profiles. Formalization could impose responsibilities and control at key integration points to overcome cultural biases. This option allows for compliance monitoring and compliance is part of the policy change. Existing Defense Information Systems Agency (DISA) technology and systems could perform automated compliance monitoring for the registration and production of profiled information products. Role and responsibility formalization could assist to overcome organizational cultural bias and overrule user discretion for withholding information. The revised policy creates a context to understand requirements for data availability, integrity, and confidentiality. Key operational nodes as data sources could transition to registered services to information sharing for the undefined user. Option II changes the existing NCDS policy to formalize information sharing responsibilities of process owners as data producers. It circumvents the existing policy of “post all data” and is most effective if key processes are targeted. This option follows the advice of Christopher Baum, Gartner Research Group, for how the government can effectively share data. Mr. Baum advocates, “understand where the data originates,” “understand the law,” and “find common needs.”[36] Option II promotes information sharing effects through policy change, formalizing the sharing responsibility of data producers at key operational points and does not require adoption of new technology. The risk of this option is overdoing the assignment of responsibilities, with data not profiled and quality attributes not defined. Information sharing responsibilities without monitoring key operational nodes for compliance enables dependence upon the implementer and allows continuation of information control biases.

III. Determine data sharing responsibilities of data sources and technologically enable process owners with the ability to push information with a Semantic Web enabled context. Use the Semantic Web layers to enable user information markup and promote collaboration by tasks for self-synchronization. Determine integration points between organizations and develop common information objects for sharing. Formalize information sharing responsibilities of static data and allow semantic technology to control access. Allow user control of dynamic data, with posting at particular points of completeness as versions. Allow individuals to enter sharing agreements and participate in information exchange within the construct of task through machine-assisted collaboration. Use key integration points and data source responsibilities to post available information as services with standardized metadata tagging and registered services. Process owners are aware of their information sharing responsibilities as with Option II. Option III requires oversight of data standards, especially for metadata tagging, developing service registries, and advancing machine collaboration tools to improve information sharing and manage information control bias. This option is most likely where the WWW and the DoD will evolve. The issue for the DoD is the immaturity of many elements of Semantic Web technology (refer to Figure 1) and the lack of trained people. The risk adverse path would allow the technology to mature in the commercial sector and transition implemented technology to the DoD.

Recommendations and Conclusions

A recommendation to adopt Option II and work towards Option III is probably the best strategy to address DoD's cultural biases and enable a culture change. Option II addresses the issue of information control directly and imposes sharing responsibilities on organizations and individuals by task and process. With the monitoring of information output at key integration points, policy compliance is checked. Technology can be an enabler for information sharing, but concentrating on technology will allow organizations and individuals to circumvent sharing responsibilities. Instead, an emphasis on Option II avoids the issue of technical maturity and transition from legacy systems. Pursuing Option II creates immediate effects and a way to build out in a modular implementation. As technology is developed and implemented in the WWW and DoD's systems, Option II only becomes stronger. An over-emphasis on technology creates another excuse to delay behavior modification and effect change.

Using the USAWC Strategy Model of “ends, ways, and means,” changing the DoD’s NCDS and other policies as a way could be one of the more immediate and effective ways to counter DoD’s cultural bias for information control. Overcome information control through determining responsibilities of data producers and assigning key operational nodes with sharing responsibilities. Monitor data producers for their compliance with the type and frequency of data products. Understanding requirements of ownership, access, classification, and other data quality attributes become enablers for understanding information sharing, instead of elements playing into cultural biases for information control. In an increasingly complex and interdependent world, this policy change is required for effective joint, interagency, and coalition information sharing. Formalizing information sharing responsibilities requires addressing numerous technical and managerial information challenges. Technical challenges of exponentially growing volumes of data, developing proper information context, and promoting accessibility and discoverability of information exists and will be with us for years. Understanding a balance of the human, policy, process, and technology is critical for implementing this future vision, as “it is essential that policy and technology be designed with a good understanding of the implications of each other.”[37]

Endnotes

[1] Government Accountability Office, “Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.” GAO-06-385, (Washington, D.C: March 2006), 2-3.

[2] Strategic Studies Institute, U.S. Army War College Key Strategic Issues List, (Carlisle Barracks, PA: July 2007), 53.

[3] Assistant Secretary of Defense for Networks and Information Integration, DoD Directive 8320.2, “Data Sharing in a Net-Centric Department of Defense” (Washington, DC: 2 December 2004), 2.

[4] Harry R. Yarger, "Toward a Theory of Strategy: Art Lykke and the Army War College Strategy Model" (Carlisle Barracks, PA: June 2006), 111.

[5] Tim Berners-Lee and Mark Fischetti, Weaving the Web, (New York: HarperCollins Books, 2000), 124.

[6] The White House, The National Security Strategy of the United States of America (Washington, DC: October 2006), 24.

[7] The White House, The National Strategy for Maritime Security (Washington, D.C.: September 2005), 13-16.

[8] Chairman of the Joint Chiefs of Staff, National Strategy to Combat Weapons of Mass Destruction (Washington, DC: 13 February 2006), 5-26.

[9] DoD Directive 8320.2, 2.

[10] Assistant Secretary of Defense for Networks and Information Integration, DoD Directive 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing" (Washington, DC 12 April 2006), 9.

[11] Assistant Secretary of Defense C3I, DoD Directive 8500.1, "Information Assurance" (Washington, DC: 24 October 2002), 4.

[12] Assistant Secretary of Defense for Networks and Information Integration, DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" (Washington, DC: 5 May 2004), 3.

[13] DoD Directive 8320.02-G, 11.

[14] Ibid, 32.

[15] Ibid, 26.

[16] The Privacy Act of 1974, 5 U.S.C. § 552a, As Amended, (Washington, DC), 464.

[17] National Institute of Standards and Technology, FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems (Gaithersburg, MD: February 2004), 1.

[18] DoD Directive 8320.2, 2.

[19] Rob Fay, "Effective Culture Change in the FBI" (15 June 2005), 2-3.

[20] Department of Homeland Security, Securing Our Homeland U.S Department of Homeland Security Strategic Plan (Washington, DC: February 2004), 6.

[21] Melvin E. Conway, "How Do Committees Invent." Datamation. (April 1968), 8.

[22] Rob Fay, 5-6.

[23] Carlos E. Cortés, "Leadership Qualities in a Changing America," Federal Executive Institute Presentation (Charlottesville, VA: March 2006), 1.

[24] Christopher Thomas and Milton Ospina, Measuring Up The Business Case for GIS (Redlands, CA: ESRI Press. 2004), 18-20.

[25] Weaving the Web, 207.

[26] Ibid, 237.

[27] Tim Berners-Lee, "Semantic Web on XML," XML 2000 (Washington DC: 6 December 2000), 17.

[28] Weaving the Web, 189-190.

[29] Ibid, 188.

[30] Director of National Intelligence, Intelligence Community Enterprise Architecture: IC EA Conceptual Data Model Version 1.2 (Washington, DC: 22 August 2006), 32.

[31] Paul Shaw, "Semantics of Security," Systems and Software Technology Conference Presentation (Salt Lake City, UT: April 2006), 7.

[32] Department of Homeland Security, "Fact Sheet: Homeland Security Operations Center (HSOC)" (Washington, DC: 8 July 2004), 1.

[33] Paul Shaw and David Roberts, "White Paper on the Cross-domain Information Exchange Framework (CIEF): Implementing the Universal Core" (San Diego, CA: 14 September 2007), 7.

[34] Melvin E. Conway, 7.

[35] Edgar M. Johnson, Workshop Introducing Innovation and Risk: Implications of Transformation the Culture of DoD, (Alexandria, VA: Institute for Defense Analyses, 2004), II-2.

[36] Christopher H. Baum, "Government Agencies are Data Stewards, Not Owners." (Stamford, CT: Gartner Research: 31 December 2004), 4-5.

[37] Weaving the Web, 124.